Claims

1. A method of managing the secure mutual configuration of a plurality of servers interconnected by a communications network, said method comprising the steps of:

a) routinely exchanging status messages between said plurality of servers wherein said status messages identify changes in the mutual configuration of said plurality of servers, wherein each said status message includes encrypted validation data and wherein said plurality of servers stores respective configuration data including respective sets of data identifying the servers known to the respective servers as constituting said plurality of servers;

b) validating status messages as respectively received by said plurality of servers against the respective configuration data stored by said plurality of servers wherein status messages are determined valid when originating from a first server as determined known relative to the respective configuration data of a second server; and

c) selectively modifying the respective configuration data of said second server.

2. The method of Claim 1 wherein said step of selectively modifying includes the steps of:

a) retrieving the respective configuration data of said first server; and

b) incorporating the respective configuration data of said first server as the respective configuration data of said second server.

3. The method of Claim 2 wherein the respective configuration data of said first server includes encrypted validation data and wherein said step of retrieving includes the step of validating the respective configuration data of said first server as originating from a known server of said plurality of servers as determined relative to the respective configuration data of a second server.

4. The method of Claim 3 wherein said known server is said first server.

5. The method of Claim 4 wherein the encrypted validation data included in the respective configuration data is a digital signature of the respective configuration data.

6. The method of Claim 5 wherein the encrypted validation data included in the status messages includes an encrypted identifier of the respective servers originating the status messages.

7. The method of Claim 6 the method of Claim 6 wherein the respective configuration data includes respective sets of the public keys corresponding to the servers known to the respective servers as constituting said plurality of servers.

8. The method of Claim 7 wherein the status messages include respective configuration data version identifiers and wherein said step of retrieving is responsive to configuration data version identifiers that are more current the configuration data version identifier of the respective configuration data held by a respective server of said plurality of servers.

9. The method of Claim 8 wherein a predetermined server of said plurality of servers includes an administrative interface through which the respective configuration data may be modified, said method further comprising the step of revising the respective configuration data version identifier of administratively modified configuration data.

10. A method of securely distributing configuration data over a communications network to a plurality of computer systems, each computer system operating to evaluate configuration data, as stored in respective configuration data stores, in response to service requests to determine respective responses, said method comprising:

a) receiving, by a computer system, a version message from said communications network;

b) verifying said version message using verification encryption data securely held by said computer system;

c) determining, based on said version message, to retrieve updated configuration data from a configuration data source server identified relative to said a version number message; and

d) installing updated configuration data to the configuration data store of said computer system as retrieved from said configuration data source server, wherein said updated configuration data is retrieved as an encrypted data block and wherein said step of installing includes locating predetermined configuration data within said encrypted data block and decrypting said predetermined configuration data.

11. The method of Claim 10 wherein said locating step determines the location of said predetermined configuration data using location encryption data securely held by said computer system.

12. The method of Claim 11 wherein said verification encryption data and said location encryption data are related to a private encryption key securely held by said computer system.

13. The method of Claim 12 wherein said verification encryption data and said location encryption data are related to respective private encryption keys securely held by said computer system.

14. The method of Claim 10 wherein said plurality of computer systems use a common version of said configuration data, wherein said step of installing finally installs said updated configuration data for use by said computer system and wherein said method further comprises the steps of:

a) staging said updated configuration data pending completion of the installation of said updated configuration data; and

b) waiting for said plurality of computer systems to signal use of a common version of said configuration data whereupon said step of installing completes the installation of said updated configuration data.

15. The method of Claim 14 wherein said computer system receives version message from each of the other ones of said plurality of computer systems,

wherein said step of determining determines the latest version of configuration data in use or staged for use by each of the other ones of said plurality of computer systems, and wherein said step of waiting waits for each of the other ones of said plurality of computer systems to signal use of a common latest version of said configuration data.

16. The method of Claim 15 wherein said plurality of computer systems to signal use of a common latest version of said configuration data through respective version messages.

17. A method of securely distributing configuration information through a communications network among a cluster of computer systems providing a network service, wherein configuration information modifications are distributed from a computer system participating in the cluster and mutually coordinated in installation in the participating cluster computer systems to enable a consistent configuration information versioned operation of said cluster of computer systems, said method comprising:

a) receiving a modified configuration data set having a predetermined configuration version;

b) preparing an encrypted configuration data set by encrypting said modified configuration data set using predetermined encryption keys corresponding to encryption key data included in said modified configuration data set;

c) sending a configuration version message, referencing said predetermined configuration version, over the communications network connecting the cluster of computer systems;

d) servicing requests to retrieve a copy of said encrypted configuration data set; and

e) coordinating, among the cluster of computer systems, installation of said modified configuration data set as the operative configuration data set of the computer systems of the cluster.

18. The method of Claim 17 wherein the computer systems of said cluster respectively execute a common network service application, wherein execution of said common network service application is dependent on a respective installed configuration data set, and wherein said step of coordinating provides for the mutually corresponding installation of said modified configuration data set by said computer systems whereby execution of said common network service application is consistent across the cluster of computer systems.

19. The method of Claim 18 wherein said modified configuration data set includes individual configuration data sets identified with respective computer systems of the cluster, wherein said modified configuration data set includes a plurality of private encryption keys and wherein said step of preparing provides for the encryption of said modified configuration data using said plurality of private encryption keys.

20. The method of Claim 19 wherein said individual data sets are encrypted relative to respective ones of said plurality of private encryption keys and wherein a predetermined computer system of said cluster must have a respective one of said plurality of private encryption keys to decrypt a corresponding one of said individual data sets from said encrypted configuration data set.

21. A method of securely distributing configuration data sets among server computer systems of a server cluster, wherein an operative configuration data set is used by an individual server computer system to define the parameters for executing a network service by that server computer system, said method comprising the steps of:

a) identifying, by a first server computer system of said server cluster, a revised configuration data set held by a second server computer system of said server cluster;

b) retrieving, by said first server computer system, said revised configuration data set from said second server computer system;

c) decrypting said revised configuration data set for installation as a current configuration data set for said first server computer system, said revised configuration data set having been uniquely encrypted for decryption by said first server computer system;

d) verifying, by said first server computer system, that each server computer system of said server cluster has said current configuration data set; and

e) installing said current configuration data set on said first server computer system as the operative configuration data for said first server computer system.

22. The method of Claim 21 wherein said revised configuration data set includes a plurality of respectively encrypted current configuration data sets and wherein said step of decrypting includes the steps of:

a) locating said current configuration data set, as encrypted uniquely for said first server computer system, from among said plurality of respectively encrypted configuration data sets; and

b) discretely decrypting said current configuration data set from said revised configuration data set.

23. The method of Claim 22 wherein said first server computer system has a unique private decryption key and wherein said step of locating depends on the identification, by said first server computer system, of a representation of said unique private decryption key in said revised configuration data set, whereby location and decryption of said plurality of respectively encrypted current configuration data sets is locked to the respective server computer systems of said server cluster.

24. The method of Claim 23 wherein said revised configuration data set includes representations of the unique private decryption keys of the respective server computer systems of said server cluster and wherein said step of locating includes:

a) matching a predetermined representation of said unique private decryption key of said first server computer system with a corresponding one of said representations of said revised configuration data set; and

b) determining, based on the matched representation of said unique private decryption key of said first server computer system, the location of said current configuration data set, as encrypted, from among said plurality of respectively encrypted configuration data sets.

25. The method of Claim 24 wherein said representations of the unique private decryption keys are secure digests of the unique private decryption keys of the respective server computer systems of said server cluster.

26. The method of Claim 21 wherein said operative configuration data set includes a first version identifier and wherein said step of identifying includes:

a) receiving, by said first server computer system, version messages from the other server computer systems of said server cluster, wherein each version message includes a second version identifier and identifies a version message source server computer system; and

b) determining, with respect to a predetermined version message, whether said second version identifier, relative to said first version identifier, corresponds to said revised configuration data set.

27. The method of Claim 26 wherein said step of identifying further includes a step of validating said version messages with respect to said first server computer system.

28. The method of Claim 27 wherein said first server computer system has a unique private decryption key and wherein said step of validating depends on the

identification, by said first server computer system, of a representation of said unique private decryption key in said version messages such that version messages lacking said representation are discarded by said first computer server computer system.

29. The method of Claim 28 wherein said version message includes representations of the unique private decryption keys of the respective server computer systems of said server cluster and wherein said step of validating includes matching said representation of said unique private decryption key of said first server computer system with a corresponding one of said representations of said revised configuration data set.

30. The method of Claim 29 wherein said representations of the unique private decryption keys are secure digests of the unique private decryption keys of the respective server computer systems of said server cluster.

31. The method of Claim 30 wherein said revised configuration data set includes said representations of the unique private decryption keys and a plurality of respectively encrypted current configuration data sets, wherein said step of decrypting includes the steps of:

a) matching, by said first server computer system, of said predetermined representation of said unique private decryption key of said first server computer system in said revised configuration data set;

b) determining, based on the matched representation of said unique private decryption key of said first server computer system, the location of said

current configuration data set, as encrypted, from among said plurality of respectively encrypted configuration data sets; and

c) discretely decrypting said current configuration data set from said revised configuration data set, whereby the location and decryption of said plurality of respectively encrypted current configuration data sets is locked to the respective server computer systems of said server cluster.

32. A server computer system coupleable through a communications network as part of a computer system cluster to support performance of a network service on behalf of a client computer system, said server computer system comprising:

a) a processor operative to execute control programs; and

b) a service program operative, through execution by said processor as a control program,

to generate responses to predetermined client requests,

wherein responses are generated based on an evaluation of an installed configuration data set,

said service program being further operative to implement a secure network protocol, interactive with said computer system cluster, to identify and receive an updated configuration data set for installation as said installed configuration data set,

said service program including a unique private encryption key,

wherein said secure network protocol provides for the transfer of an encrypted configuration data block including a plurality of encrypted updated configuration data sets, a respective one of said plurality of encrypted updated data sets being decryptable using said unique private encryption key.

33. The server computer system of Claim 32 wherein said service program is operative to first locate and second decrypt said respective one of said plurality of encrypted updated data sets based on said unique private encryption key.

34. The server computer system of Claim 33 wherein said encrypted configuration data block includes a plurality of location references, wherein said service program is operative to associate said unique private encryption key with a corresponding one of said plurality of location references, said service program being further operative to locate said respective one of said plurality of encrypted updated data sets based on said corresponding one of said plurality of location references.

35. The server computer system of Claim 34 wherein said corresponding one of said plurality of location references is a secure digest of said unique private encryption key.

36. The server computer system of Claim 34 wherein said service program is operative to determine whether to receive said updated configuration data set.

37. The server computer system of Claim 36 wherein said installed configuration data set has a first version identifier, wherein said updated configuration data set has a second version identifier, said service program being responsive to said first and second version identifiers to determine whether to receive said updated configuration data set.

38. The server computer system of Claim 37 wherein said service program is operative, in response to administrative modifications that produce said updated configuration data set, to generate said encrypted configuration data block with said second version identifier, said service program being further operative to provide a version message containing said second version identifier to said computer system cluster and responsive to requests to transfer said encrypted configuration data block.

39. The server computer system of Claim 37 wherein said service program is operative to successively broadcast said version message.

40. The server computer system of Claim 39 further comprising a first network connection coupleable to said client computer system and a second network connection coupleable to said computer system cluster, wherein said second network connection is utilized to successively transfer said version message and to transfer said encrypted configuration data block.

41. The server computer system of Claim 40 further comprising a third network connection accessible by an administrator for applying administrative modifications that produce said updated configuration data set.

42. A method of securely constraining participation of select computer systems in the cooperative operation of a server cluster to insure the integrity of the

information transactions among the computer systems of said server cluster, said method comprising the steps of:

a) receiving, by a first computer system of a server cluster, a request for the transfer of first specified data, held in a first secure memory store of said first computer system, to a second computer system of said server cluster;

b) transmitting, by said first computer system, encrypted information including said first specified data to said second computer system, wherein said encrypted information, as prepared by said first computer system, is further encoded to include a first secure discrete reference;

c) verifying said first secure discrete reference against a second secure discrete reference determinable from second specified data stored in a second secure memory store of said second computer system;

d) locating, by said second computer system with respect to said first secure discrete reference, a predetermined subset of said encrypted information decryptable by said second computer system to recover said first specified data; and

e) installing said first specified data in said second secure memory store of said second computer system.

43. The method of Claim 42 wherein said request and said encrypted information are transferred over a communication network interconnecting the computer systems of said server cluster.

44. The method of Claim 43 wherein said first and second secure discrete references are secure digests of a secure private encryption key assigned to said second computer systems.

45. The method of Claim 44 wherein said first and second specified data respectively includes said first and second secure discrete references.

46. The method of Claim 44 wherein said first and second specified data includes said secure private encryption key.

47. The method of Claim 44 wherein each of the computer systems of said server cluster are assigned unique secure private encryption keys and wherein a set of secure discrete references, including said first and second secure discrete references, corresponding to the set of unique secure private encryption keys are determinable from the respective specified data stored by said computer systems of said server cluster.

48. The method of Claim 47 wherein the set of unique secure private encryption keys are stored in each of the respective specified data stored by said computer systems of said server cluster.

49. The method of Claim 47 wherein the respective specified data stored by said computer systems of said server cluster are versioned, said method further comprising the steps of:

a) identifying, by said second computer system, that said first specified data is a later version relative to the version of said second specified data; and

b) requesting, by said second computer system, said first specified data from said first computer system.

50. The method of Claim 49 further comprising the step of coordinating, relative to others of said computer systems of said server cluster, the installation of said first specified data by said second computer system.

51. The method of Claim 50 wherein said step of identifying further identifies said first specified data as the latest available version of the respective specified data.

52. The method of Claim 50 wherein said second computer system nominally responds to predetermined client requests, said method further comprising the step of declining, by said second computer system, said predetermined client requests in the interim between said step of identifying and said step of installing.

53. A method of distributing configuration control data among a cluster of computer systems to ensure consistent operation of the cluster in response to network requests received from host computers, wherein each computer system maintains a local control data set that, in active use, determines the functional operation of the respective computer system, and wherein said cluster of computer systems and said host computers are interconnected by a communications network, said method comprising the steps of:

a) storing, in a first computer system of a cluster of computer systems, a first local control data set having a predetermined version number;

b) transmitting a cluster message including said predetermined version number from said first computer system to said cluster of computer systems;

c) transferring said first local control data set to requesting computer systems of said cluster of computer systems; and

d) synchronizing with said requesting computer systems the installation of said first local control data set for active use by said requesting computer systems.

54. The method of Claim 53 further comprising the step of changing said predetermined version number in connection with a predetermined modification of said first local control data set, wherein said requesting computer systems are responsive to the change in said predetermined version number.

55. The method of Claim 54 wherein said step of synchronization includes the steps of:

a) providing, respectively by said requesting computer systems, readiness signals to said cluster to establish a readiness to install said first local control data set; and

b) establishing, respectively by said requesting computer systems, receipt of said readiness signals from all of said requesting computer systems to enable respective installation of said first local control data set for active use.

56. The method of Claim 55 wherein each actively participating computer system of said cluster routinely performs said step of transmitting, wherein each

actively participating computer system may be a requesting computer system relative to any other participating computer system that transmits a cluster message with a relatively more recently predetermined version number, wherein said readiness signals include respective predetermined version numbers, and wherein said step of establishing converges on a common predetermined version number.

57. The method of Claim 56 wherein said cluster messages securely circumscribe said actively participating computer systems relative to said respectively transmitting computer systems.

58. The method of Claim 57 wherein said readiness signals include respective cluster messages.

59. A method of enabling the secure, consistent, single-point management of the individual computer system configurations within a cluster of computer systems provided to perform a common network service in response to network requests provided by host computers, wherein said cluster of computer systems and said host computers are interconnected by a communications network, said method comprising the steps of:

a) providing each of said computer systems of said cluster with a active configuration data set that operatively defines the respective operation of said computer system with respect to network requests received from host computers, wherein said active configuration data sets are represented by predefined version values;

b) transmitting, mutually among said computer systems of said cluster, cluster messages including respective representations of said predefined version values;

c) supporting, with respect to a predetermined computer system of said cluster, provision of a updated configuration data set for installation as said active configuration data set, said updated configuration data set having an updated version value, and wherein said cluster messages transmitted by said predetermined computer system reflect said updated version value;

d) propagating said updated configuration data set from said predetermined computer system among said computer systems of said cluster; and

e) coordinating the installation of said updated configuration data set as said active configuration data set in each of said computer systems of said cluster.

60. The method of Claim 59 wherein said step of coordinating provides for the installation of said updated configuration data set determined respectively based on a convergence of the version values received in said cluster messages from the computer systems of said cluster.

61. The method of Claim 60 wherein said provision of said updated configuration data set includes administrative provision.

62. The method of Claim 61 wherein said provision of said updated configuration data set includes a modification of the local active configuration data set.

63. The method of Claim 62 wherein said step of coordinating provides for the respective installation of said updated configuration data set by the computer systems of the cluster once a respective computer system receives a predetermined number of said cluster messages from each of the other computer systems of said cluster each including said updated version value.

64. The method of Claim 63 wherein said predetermined number is two.

65. A method of securely establishing consistent operation of a networked cluster of computer systems to provide a network service on behalf of host computer systems, said method comprising the steps of:

a) enabling distribution of an updated configuration data set among a cluster of computer systems, wherein each said computer system is operative against a respective active configuration data set, and wherein respective instances of said updated configuration data set are received and held by said cluster of computer systems pending installation as said respective active configuration data sets;

b) determining, by each said computer system, when a predetermined installation criteria is met with respect to each said computer system; and

c) installing said respective instances of said updated configuration data set as said respective active configuration data sets.

66. The method of Claim 66 wherein said step of enabling distribution includes a step of transmitting a message to said cluster of computer systems and wherein

said message is encrypted so as to be readable only by those computer systems of said cluster that are predetermined valid participants in said cluster.

67. The method of Claim 67 wherein said message, as prepared by a first computer systems of said cluster, is encrypted so as to be readable only by second computer systems of said cluster that are preestablished to said first computer system as valid participants of said cluster.

68. The method of Claim 68 further comprising the step of preparing, by said first computer system, said message utilizing encryption codes respectively corresponding to said second computer systems.

69. The method of Claim 69 wherein said first computer system securely stores a preestablished set of public key encryption codes corresponding to said second computer systems and wherein said second computer systems are only responsive to said message where said message stores a secure representation of the respective public key encryption code of a corresponding one of said second computer systems that receives said message.

70. The method of Claim 65 further comprising the steps of:

a) storing, by a first computer system of said cluster, a set of encryption codes corresponding to second computer systems of said cluster, said set of encryption codes being preestablished, representing predetermined valid participants in said cluster, and securely stored by said first computer system;

b) preparing, by said first computer system, a message for distribution to said second computer systems, said message including secure representations of said encryption codes;

c) transmitting said message to said cluster; and

d) validating said message by said second computer systems upon recognizing respective instances of said representations of said encryption codes.

71. The method of Claim 70 further comprising the step of retrieving, by a predetermined second computer system, a copy of said set of encryption codes from said first computer system for use by said predetermined second computer system subsequently in the role of said first computer system.

72. The method of Claim 71 wherein said secure representations are secure hashes of the public keys of said second computer systems.

73. A method of securely constraining participation of select computer systems in the operation of a server cluster, interconnected by a communications network, to insure the security of configuration information distributed among the computer systems of said server cluster, said method comprising the steps of:

a) storing, by a first computer system of a server cluster, first specified data within a secure memory store, said first specified data being identified by a first version identifier;

b) receiving, by said first computer system, a cluster message including a second version identifier and verification data from a second computer system of said server cluster;

c) verifying, by said first computer system, said cluster message by evaluation of said verification data relative to said first specified data;

d) obtaining, from said second computer system, dependent on a successful verification of said verification data, encrypted information including second specified data corresponding to said second version identifier;

e) decrypting said second specified data from said encrypted information; and

f) incorporating said second specified data into said secure memory store of said first computer system, whereby the operation configuration of said first computer system is securely made consistent with that of said second computer system.

74. The method of Claim 73 wherein said first and second specified data is configuration information that, as incorporated in said secure memory store, determines the operational performance of said first computer system of said server cluster in responding to network requests issued by any of a plurality of host computer systems to obtain a performance of a network service.

75. The method of Claim 74 wherein said first specified data includes a predetermined set of encryption codes corresponding to the validly participating computer systems of said server cluster as known to said first computer system, and wherein said step of validating said cluster message includes requiring the valid decryption of said verification data using an encryption code of said predetermined set identified with said second computer system, whereby cluster

messages are accepted as valid by said first computer system only from preestablished validly participating computer system of said server cluster.

76. The method of Claim 75 wherein changes to said predetermined set of encryption codes are constrained to secure update procedures including incorporation of said second specified data into said secure memory store and administrative operations securely executed against a computer system of said server cluster, whereby configuration data is securely maintained and distributed only among the computer systems of said server cluster of administratively preestablished identity.

77. The method of Claim 76 wherein said verification data includes a predetermined cipher text encrypted to ensure secure identification of said request as originating from said second computer system.

78. The method of Claim 77 wherein said verification data includes a predetermined cipher text encrypted with an encryption key pair corresponding to said second computer system.

79. A computer system operable as a participant in a cluster of computer systems providing a network service in response to network requests received from host computer systems through a communications network, the cluster computer systems interoperating to ensure the security and secure exchange of configuration data in response to a single point secure administrative modification

of configuration data on any computer system of the cluster, said computer system comprising:

a) a computer memory providing for the storage of configuration data including a set of identifications of computer systems participating in a preestablished computer system cluster;

b) a processor coupled to said computer memory and operative to execute a control program that defines performance of a predetermined network service in response to network requests as received from host computers, wherein performance of said predetermined network service is controlled by said configuration data;

c) an administrative interface coupled to said processor, wherein said control program further enables secure performance of local administrative modifications to said configuration data through said administrative interface; and

d) a communications interface coupled to said processor and coupleable to said preestablished computer system cluster, wherein said control program further enables secure synchronization of said configuration data among said computer system and said preestablished computer system cluster, said control program limiting the transfer of said configuration data between said computer system, as a first computer system, and a second computer system securely matching a identification preexisting in said set of identifications.

80. The computer system of Claim 79 wherein said configuration data is transferred encrypted between said first computer system and said second

computer system and wherein the encryption of said configuration data is specific to said first computer system and said second computer system.

81. The computer system of Claim 80 wherein said processor is responsive to a network synchronization message identifying a configuration data set more recently modified relative to the configuration data stored in said computer memory, said processor being operative to identify said second computer system as the source of said network synchronization message, send a network configuration data request message to said second computer system. receive, and decrypt said configuration data set, and incorporate said configuration data set into said computer memory.

82. The computer system of Claim 81 wherein said processor is further operative to validate said network synchronization message relative to said set of identifications, prepare said network configuration data request to be validateable against said set of identifications, and validate said configuration data set as received against said set of identifications, whereby the transfer of said configuration data set is secure and constrained with respect to said first computer system to those computer systems of said preestablished computer system cluster that are preexistingly identified by said set of identifications.